REMARKS

Claims 1, 12, 13, 16, 17, 20, 26, 27, 31 and 34 have been amended.

Claims 1 – 36 are present in the subject application.

In the Office Action dated February 2, 2005, the Examiner has rejected claims 1 – 36 under 35 U.S.C. §103(a). Favorable reconsideration of the subject application is respectfully requested in view of the following remarks.

The Examiner has rejected claims 1 – 9, 11 – 28 and 30 – 36 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,335,276 (Thompson et al.) and further in view of U.S. Patent No. 5,940,799 (Bruckert et al.). Initially, a user may access a network by placing a call to a voice browser system. Since the user is accessing the network by telephone, voice browser systems do not have access to user security information to establish a secure session with a secure network site. Accordingly, conventional voice browser systems are unable to provide users with secure sessions. The present invention overcomes this problem and enables voice browsers to conduct a secure session for users. In particular, the present invention is directed toward a system for facilitating secure network communications including a security computer system utilized in conjunction with a voice browser residing on a server system. The present invention includes a module for a voice browser that creates a secure connection to the security system. The user provides an identification to the voice browser system that is transferred to and verified by the security system. Once the identification is verified, the user is prompted by the voice browser system to speak a phrase for voice verification. The verification speech signals are transferred from the voice browser system to the security system to verify those speech signals against speech signals of a particular authorized user associated with the identification

and stored in a database. When the user is verified, the security system retrieves a user private key and certificate from the database. In response to the user subsequently accessing a web site residing on a secure server, the secure server and voice browser system initiate a secure key exchange. Data packets containing security information are transferred from the voice browser system to the security system for processing, while security information from the security system is transferred to the secure server via the voice browser system. The resulting session key is securely transferred to the voice browser system to facilitate secure communications between the voice browser system and secure server. In other words, the security system handles processing of the security information from the secure web site to enable the voice browser to conduct a secure session with that site.

The Examiner takes the position that the Thompson et al. patent discloses all the features within these claims except for a retrieval module to retrieve security information of a verified user from a storage unit and a negotiation module to negotiate communication parameters with a secure network site utilizing the retrieved security information in response to receiving identified security information from a security module to facilitate secure communications over the network between that site and the network interface. The Examiner further alleges that the Bruckert et al. patent teaches these features and that would it have been obvious to combine the teachings of the Thompson et al. and Bruckert et al. patents to attain the claimed invention.

This rejection is respectfully traversed since the Thompson et al. and the Bruckert et al. patents, either alone or in combination, do not disclose, teach or suggest a security system to handle processing of security information from a secure network site to enable a voice responsive interface to conduct secure communications as recited in the claims. However, in

order to expedite prosecution of the subject application, independent claims 1, 12, 16, 20, 31 and 34 have been amended to further clarify these features. In particular, independent claims 1, 12, 16 and 20 have been amended and recite the features of: a security module identifying security related information received by a network interface from a secure web site in response to a voice browser accessing the secure web site based on voice commands from a user, wherein the security related information includes information enabling a secure session with the secure web site; voice and security information remotely stored from the network interface with the security information including information enabling negotiation of parameters for secure sessions with secure web sites; a security system processing the identified security information for the network interface and receiving the identified security information from the security module and negotiating communication parameters with the secure web site utilizing the retrieved security information to facilitate the secure session between that site and the voice browser. Independent claims 31 and 34 have been amended and recite the features of: retrieving security information of a verified user, including information enabling secure sessions with secure web sites, remotely stored from the network interface and negotiating communication parameters for the network interface with a secure web site accessed by a voice browser utilizing the retrieved security information to facilitate a secure session between that site and the voice browser in response to the voice browser accessing the secure web site based on voice commands from the user.

The Thompson et al. patent does not disclose, teach or suggest these features. Rather, the Thompson et al. patent discloses a communication system provided with multiple-purpose personal communication devices. Each communication device includes a touch-sensitive visual display to communicate text and graphic information to and from the user and for operating the communication device. Voice activation and voice control capabilities are included within the

communication devices to perform the same function as the touch-sensitive visual display. A plurality of application modules are used with the personal communication devices to perform a wide variety of communication functions, such as information retrieval, on-line database services, electronic and voice mail (e.g., See Abstract). A digital signal processor allows voice verification of a communication device user, where the voice verification information may be stored at a central facility or within the digital signal processor. This ensures that only authorized users are sending and receiving information over a communication network (e.g., See Column 17, lines 62 - 68). The user may utilize voice commands to activate a selected communication application and communicate with the central facility that provides secure communications by encryption and decryption of transmitted information. The central facility will broadcast highly sensitive, valuable information in a coded format to the communication device with a high degree of confidence that only an authorized user of the communication device will receive the information (e.g., See Column 17, line 68 to Column 18, line 8).

Thus, the Thompson et al. patent discloses a universal communication device capable of performing various functions. Although the communication device provides voice activation and voice verification to enable encryption and decryption of transmitted information, there is no disclosure, teaching or suggestion of enabling a secure session between a voice browser and a secure web site or, for that matter, identifying security related information received in a voice responsive network interface from a secure web site (e.g., Claims 1, 12, 16 and 20), storing security information of the user remotely from the network interface (e.g., Claims 1, 12, 16, 20, 31 and 34) wherein the security information includes information enabling negotiation of parameters for secure sessions with secure web sites (e.g., Claims 1, 12, 16 and 20) or a security system or negotiation unit negotiating communication parameters with the secure web site for

the network interface to enable a secure session between the voice browser and the web site (e.g., Claims 1, 12, 16, 20, 31 and 34) as recited in the independent claims.

The Bruckert et al. patent does not compensate for the deficiencies of the Thompson et al. patent and similarly does not disclose, teach or suggest these features. Rather, the Bruckert et al. patent discloses a processing system that is accessible via a number of speech transmission media. Access to the processing system may be made via a mobile radio telephone, land line telephone, acoustic link or data link. Access to programs, files and data is based upon the security of the communication media and authentication of the user (e.g., See Abstract).

Although the Bruckert et al. patent discloses speech recognition authentication and public key exchange (e.g., See Column 4, lines 31 – 34 and Column 6, lines 20 – 24), there is no disclosure, teaching, or suggestion of a security system or negotiation unit to negotiate communication parameters with a secure web site for a network interface to enable a secure session between a voice browser and that web site as recited in the independent claims. In fact, the Bruckert et al. patent does not disclose, teach or suggest identifying security related information received at the network interface wherein the security information includes information to establish a secure session with the web site (e.g., Claims 1, 12, 16 and 20), remotely storing user security information from the network interface (e.g., Claims 1, 12, 16, 20, 31 and 34) wherein the user security information enables secure sessions with secure web sites (e.g., Claims 1, 12, 16 and 20), or a security system or negotiation unit negotiating communication parameters with the secure web site for the network interface to enable a secure session between the secure web site and voice browser (e.g., Claims 1, 12, 16, 20, 31 and 34) as recited in the independent claims.

Since the Thompson et al. and Bruckert et al. patents do not disclose, teach or suggest, either alone or in combination, the features recited in independent claims 1, 12, 16, 20, 31 and 34 as discussed above, these claims are considered to be in condition for allowance.

Dependent claims 2 – 9, 11, 13 – 15, 17 – 19, 21 – 28, 30, 32 – 33 and 35 – 36 depend, either directly or indirectly, from independent claims 1, 12, 16, 20, 31 or 34 and, therefore, include all limitations of their parent claims. Claims 7, 13, 17 and 26 - 27 have been amended for consistency with their amended parent claims. The dependent claims are considered to be in condition for allowance for substantially the same reasons discussed above in relation to their parent claims and for further limitations recited in the dependent claims.

The Examiner has rejected claims 10 and 29 under 35 U.S.C. §103(a) as being unpatentable over the combination of the Thompson et al. and Bruckert et al. patents and further in view of U.S. Patent No. 5,341,426 (Barney et al.). Briefly, the present invention is directed toward a system for facilitating secure network communications including a security computer system utilized in conjunction with a voice browser residing on a server system as described above.

The Examiner takes the position that the combination of the Thompson et al. and Bruckert et al. patents discloses all of the features within these claims except for stored security information including private keys and certificates of authorized system users. The Examiner further alleges that the Barney et al. patent discloses these features and that it would have been obvious to combine the Thompson et al., Bruckert et al. and Barney et al. patents to attain the claimed invention.

This rejection is respectfully traversed. Initially, claims 10 and 29 respectively depend, either directly or indirectly, from independent claims 1 and 20 and, therefore, include all of the limitations of their parent claims. As discussed above, the combination of the Thompson et al. and Bruckert et al. patents does not disclose, teach or suggest the features of identifying security related information received at a network interface from a secure web site wherein the security information includes information enabling a secure session, remotely storing user security information from the network interface wherein the user security information includes information enabling negotiation of parameters for secure sessions with secure web sites, and a security system or negotiation unit negotiating communication parameters with the secure web site for the network interface to enable a secure session between the secure web site and voice browser.

The Barney et al. patent does not compensate for the deficiencies of the Thompson et al. and Bruckert et al. patents and similarly does not disclose, teach or suggest these features. Rather, the Barney et al. patent is merely utilized by the Examiner to disclose use of public keys and certificates.

Since the Thompson et al., Bruckert et al., and Barney et al. patents do not disclose, teach or suggest, either alone or in combination, the features recited in claims 10 and 29 as discussed above, these claims are considered to be in condition for allowance.

In addition to the foregoing, there is no apparent reason or motivation to combine the teachings of the Thompson et al., Bruckert et al., and Barney et al. patents. The Thompson et al. patent is directed toward a universal communication device as described above. The Bruckert et al. patent is directed toward access of a remote computer system as described above, while the

Barney et al. patent discloses use of keys and certificates for secure connections as described above. Thus, the patents are directed toward diverging applications and there is no apparent reason, motivation or suggestion to combine their teachings absent prohibited hindsight derived from Applicant's own disclosure. Accordingly, the proposed combinations of the Thompson et al., Bruckert et al., and Barney et al. patents do not render the claimed invention obvious.

The application, having been shown to overcome the issues raised in the Office Action, is considered to be in condition for allowance and a Notice of Allowance is earnestly solicited.

Respectfully submitted,

Stuart B. Shapiro
Registration No. 40,169

EDELL, SHAPIRO & FINNAN, LLC
1901 Research Boulevard, Suite 400
Rockville, Maryland 20850-3164
(301) 424-3640

Hand Delivered: APRIL 29, 2005